California
Department of Technology
California Information Security Office

Incident Management Program Resources

Resources

INCIDENT MANAGEMENT PROGRAM RESOURCES

- Inter-Agency Security Group
  - Comprised of state employees whose job duties deal directly or indirectly with information security
  - Meet every second Thursday of every EVEN Month
  - Open for State employees only
  - To join, contact Helen Woodman of CISO
    - (916) 431-4698 or helen.woodman@state.ca.gov

- Multi-State Information Sharing and Analysis Center (MS-ISAC)
  - *Free* services available to state, local, tribal and territorial governments
    - Malware Analysis, Computer Forensics, Network Forensics, Incident Response, and Onsite Assistance
  - Contact Information to request services
    1-866-787-4722 or soc@msisac.org

- Malicious Code Analysis Platform (MCAP) service
  - Request account by emailing mcap@cisecurity.org
  - Once account is created, you may login and upload the file for analysis at https://mcap.cisecurity.org/
  - *Free* education and awareness material
    https://www.cisecurity.org/training/

- Websites to test for systems vulnerable to DDoS:
  - http://openresolverproject.org/ (Open Resolvers – DNS)
  - http://openntpproject.org/ (NTP)
  - http://openssdpproject.org/ (Simple Service Discovery Protocol)
  - http://opensnmpproject.org/ (SNMP)

Resources

- Department of Justice, Privacy Enforcement and Protection Unit
  - www.privacy.ca.gov

- United States Computer Emergency Readiness Team (US-CERT)
  - http://www.us-cert.gov/
  - Forum of Incident Response and Security Team (FIRST)
  - www.first.org

- SANS
  - www.sans.org
  - Critical Log Review Checklist for Security Incidents
  - SANS Incident Handler's Handbook
  - http://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

- National Cyber Security Alliance
  - *Free* education and awareness material www.staysafeonline.org

- NIST SP
  - http://csrc.nist.gov/publications/PubsSPs.html
    - NIST SP 800-61, Computer Security Incident Handling Guide
    - NIST SP 800-83, Malware Incident Prevention and Handling
    - NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, which includes sample incident response exercises

Resources

- Texas A&M Engineering Extension Service
  - Free online courses
  - Choose Course Option: Cybersecurity
  - https://teex.org/Pages/Program.aspx?catID=231&courseTitle=Cybersecurity
  - CYB101 - Cybersecurity for Everyone – Non-Technical
    - AWR-168-W Cyber Law and White Collar Crime
    - AWR-174-W Cyber Ethics
    - AWR-175-W Information Security for Everyone
  - CYB201 - Cybersecurity for IT Professionals - Technical
    - AWR-138-W Network Assurance
    - AWR-139-W Digital Forensics Basics
    - AWR-173-W Information Security Basics
    - AWR-178-W Secure Software
  - CYB301 - Cybersecurity for Business Professionals/Managers
    - AWR-169-W Cyber Incident Analysis and Response
    - AWR-176-W Business Information Continuity
    - AWR-177-W Information Risk Management

- Carnegie Mellon University
  - Papers on Incident Management http://resources.sei.cmu.edu/library/results.cfm?as_q=inmeta:gsataxonomyoutput~Incident%20Management

Resources

- Department of Homeland Security
  - Office of Cybersecurity & Communications
  - Cyber Education and Awareness Branch
  - DDoS Quick Guide
  - https://www.us-cert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf

- Federal Virtual Training Environment (FedVTE)
  - https://fedvte.usalearning.gov/
  - Available to state, local, tribal and territorial governments
  - No cost to users
  - online and on-demand cybersecurity training system
  - Courses ranging from beginner to advanced levels
  - Accessible from most common web browsers.